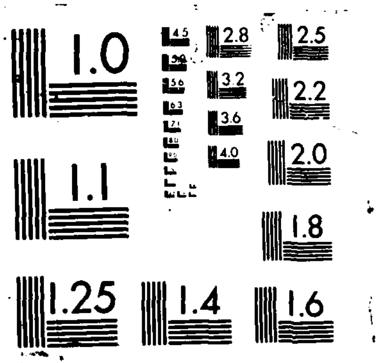
AD-A187 201 ADP SECURITY STANDING OPERATING PROCEDURES(U) ARMY 1/1
TRADOC ANALYSIS COMMAND FORT LEAVENWORTH KS
W R DONEHUE 30 SEP 87 TRAC-F-TM-1187

UNCLASSIFIED F/G 12/8 NL


1.0
4.5
5.0
5.6
6.3
7.1
8.0
9.0
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.1
1.8
1.25
1.4
1.6

Technical Memorandum TRAC-F-TM-1187
September 1987

(2)

TRADOC Analysis Command-Fort Leavenworth (TRAC-FLVN)
Operations Directorate
Fort Leavenworth, Kansas 66027-5200

ADP SECURITY STANDING OPERATING PROCEDURES

by

William Donehue

ACN 27438

The views, opinions, and/or findings contained in this report are not to be construed as an official Department of the Army position, policy, or decision unless so designated by authorized documents issued and approved by the Department of the Army.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS
NONE

2a. SECURITY CLASSIFICATION AUTHORITY

3. DISTRIBUTION/AVAILABILITY OF REPORT
UNLIMITED

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE
N/A

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
TRAC-F-TM-1187

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
TRAC-FLVN/OD/CSD/IMO

6b. OFFICE SYMBOL *(If applicable)*
ATRC-FOC-I

7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS *(City, State, and ZIP Code)*
Director, TRAC-FLVN
ATTN: ATRC-FOC-I
Ft Leavenworth, KS 66027-5200

7b. ADDRESS *(City, State, and ZIP Code)*

8a. NAME OF FUNDING/SPONSORING ORGANIZATION

8b. OFFICE SYMBOL *(If applicable)*

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS *(City, State, and ZIP Code)*

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.

11. TITLE *(Include Security Classification)*
ADP Security Standing Operating Procedures

12. PERSONAL AUTHOR(S)
Donehue, William R.

13a. TYPE OF REPORT
Annual

13b. TIME COVERED
FROM 9/87 TO 9/88

14. DATE OF REPORT *(Year, Month, Day)*
87/09/30

15. PAGE COUNT
62

16. SUPPLEMENTARY NOTATION

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
ADP; Security; Procedures, Policy.

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

The ADP Security SOP provides TRAC-FLVN users of automated equipment with guidance for processing in a secure environment for the level of processing being done. The SOP also provides guidance for handling various levels of ADP media such as tapes, diskettes, and printed media. The SOP provides guidance for processing on various TRAC-FLVN networks and for handling emergency situations such as fires, floods, and bomb threats.

[illegible]

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL
Donehue, William R.

22b. TELEPHONE *(Include Area Code)*
(913) 682-5352

22c. OFFICE SYMBOL
ATRC-FOC-I

Previous editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

TABLE OF CONTENTS

Page

CHAPTER 1

ADP SECURITY STANDING OPERATING PROCEDURES

Section I. General

1. Purpose. This standing operating procedure (SOP) describes methods used to implement the Army Automation Security Program and provide security measures for the automated resources within Headquarters, TRADOC Analysis Command (TRAC), and TRAC-Fort Leavenworth (FLVN). These resources consist of automated equipment, computer and analytic facilities, and the data and information stored on the automated equipment or within these facilities.

2. Scope. This SOP is applicable to all elements of HQ, TRAC, and TRAC-FLVN to attain a consistent level of security for all the organization's automated resources. Throughout this document, any reference to TRAC-FLVN's resources also include appropriate reference to those automation resources in HQ, TRAC. This SOP applies to all users of automated systems and their supervisors. Minimum requirements are stated herein; managers, security personnel, and users are free to implement more stringent measures at their various locations after approval by the automatic data processing system security officer (ADPSSO).

3. Objective. The objective of this SOP is to set forth guidelines on safeguarding all automated information resources against unauthorized access, use, modification, manipulation, or destruction at any level, and to provide basic policies, guidelines, techniques, and procedures for TRAC-FLVN's automated resources and its remote sites. This SOP, in conjunction with Army and command policies, can be used to implement protected, dependable ADP systems which minimize the opportunity of sabotage, deliberate or inadvertent access to sensitive or classified material by unauthorized personnel, or the unauthorized manipulation of TRAC-FLVN automated systems and all associated peripheral devices. It is not intended to be an all-encompassing or exhaustive reference on security. To gain greater specificity, the cited references should be used.

4. References.

a. AR 38Ø-38Ø, Automated Systems Security.

b. AR 38Ø-5, Department of the Army Information Security Program.

c. AR 18-7, Automatic Data Processing Management Review Program.

d. TB 18-1ØØ, Acquisition of ADPE.

e. AR 18-22, Army Inventory of Data Systems.

f. DOD Regulation 5200.1, DoD Information Security Program.

g. Federal Information Processing Standards Publication (FIPS) 31. Guidelines for Automatic Data Processing Physical Security and Risk Management.

h. TB 18-108, Army Automation Continuity of Operations Plan (COOP).

5. Definitions. See glossary at appendix A.

6. Resource utilization. All TRAC-FLVN computer systems, automated information resources, and associated peripheral devices will only be used by authorized users for assigned official work. They will not be used otherwise. Personal files such as games, recipes, and sports pools are specifically prohibited by AR 380-380.

Section II. Personnel Manning and Control

1. General. The proliferation and use of high-dollar, mission-essential automation equipment in TRAC-FLVN necessitates that all personnel in the organization be aware of and promote the security of these resources. This equipment processes and stores sensitive information that is either classified or unclassified. The handling of information should be commensurate with its level of classification. Classified defense information requires the greatest deal of protection; however, there is also a large amount of unclassified, yet sensitive, information that also requires some form of control and protection. This may include certain model software, proprietary software purchased for use on various equipment, personnel and financial information, or information which is not releasable to contractor personnel. The requirements for safeguarding and storing information are as follows:

a. Unclassified (U). Materials marked "UNCLASSIFIED" do not require special treatment for handling or storage. However, even unclassified material should be regarded as potentially sensitive in nature and should be safeguarded from those who do not have a valid need to know the information.

b. For official use only (FOUO). Although not classified, materials marked FOUO should be considered sensitive in nature. Proper safekeeping may be satisfied by locking in a desk or filing cabinet, briefcase, or other locked container. Do not store FOUO materials in a classified container.

c. Restricted. Materials marked "RESTRICTED" should be handled as confidential except that they may be properly secured by locking in a desk or filing cabinet. Restricted is a special NATO classification that should be given sufficient safeguarding to prevent compromise by those without a need to know the information.

d. Confidential (C) and secret (S). Materials marked with these labels are classified which must be provided considerable care in handling and safekeeping. They must be secured in an approved classified container, such as the rotary dial safes in building 5Ø. These materials must be kept under constant surveillance and face down or covered when outside of approved containers. Do not allow classified material to remain unguarded if you are stepping out of the office, even for only a moment. They may never be stored in desks, filing cabinets, or other unapproved containers. It is best to keep classified material in-hand until no longer needed, then remove any classified document cover sheet and return the document to the safe.

e. Top secret (TS). Materials marked "TOP SECRET" may not be stored within any of TRAC's activities. Few individuals possess a TS clearance so these items must be hand carried and provided the maximum level of security possible. With proper coordination, TS material may be stored in the Classified Mailroom, located in the basement of Sheridan Hall.

f. Not releasable to foreign nationals (NOFORN). Materials marked with this classification must be provided the same level of handling and safeguarding that classified documents require. In addition, they may not be provided to foreign personnel without specific authority from the Directorate of Plans, Training, Mobilization, and Security (DPTMSEC), Security Division.

g. No contractor. Items so marked may not be provided to civilian contractor personnel without specific authority by DPTMSEC, Security Division.

h. REMEMBER. Consider all documents as sensitive. Not everyone in TRAC has a security clearance. Secure documents when no longer needed. Discuss classified information only on a need-to-know basis and never on unsecure telephone lines. When in doubt, protect information to the highest level until a proper determination can be made about its classification.

2. Responsible personnel. The commander and managers at all levels are responsible for the secure operation of automated systems and will take all actions to ensure this security. They will be assisted by automation security personnel, whose duties are discussed below.

a. Automatic data processing systems security officer (ADPSSO). The ADPSSO is the primary staff official appointed to supervise, direct, and advise both users and management of all facets of automation security. The individual will be appointed in writing by the commander, TRAC in accordance with paragraph 1-4, AR 380-380. This designation will authorize the ADPSSO to partially or completely suspend any operations which may affect the security of the system. This will also authorize the ADPSSO to suspend access to any system subscriber. These duties will be part of the individual's primary duties. These duties are outlined in appendix B.

b. Assistant ADPSSO. An assistant ADPSSO will be appointed in writing for each TRAC-FLVN computer system including office automation systems and personnel computers (PCs), other than the systems in the Central Computer Facility. The major computer systems are located in the Training Development Computer Facility in building 50W, the Wargaming Computer Facility in building 391, and the Combat Development Computer Facility in building 193, and the Battalian/Brigade Simulation Computer Facility in building 275. Appendix C provides a list of the assistant ADPSSO's duties.

c. Terminal area sec' rity officer (TASO). The TASO and alternate TASO represent and support automation security and the ADPSSO in the terminal area(s) or the office(s) containing office automation equipment. The TASO will be appointed in writing in accordance with paragraph 1-4, AR 380-380. The TASO should be an individual who is technically qualified for the system and hardware under his/her purview, and who is routinely in or near the terminal area. The functions and responsibilities are in addition to his/her primary duties, and will be designated by the director in whose area the equipment is used and operated. Appendix D outlines the TASO's responsibilities.

d. Network security officer (NSO). The NSO is responsible for all aspects of a network that processes sensitive defense information. AR 380-380, paragraph 1-4(n) provides the duties for an NSO. These duties are listed at appendix E of this document.

e. User responsibilities (all personnel). Users are to support automation security. Access to computer systems is given to users based on work assignments, need-to-know, and security clearance level. Authorized user access to computer systems constitutes an agreement on the part of the user to maintain a secure environment while processing sensitive data and to handle removable media (e.g., magnetic tapes/disks, printouts, etc.) according to its level of classification. Computer systems accessed by users will be used for official government business only. All personnel are responsible to report known or suspected security violations to the ADPSSO and/or the assistant ADPSSO. Security personnel cannot be everywhere all the time; without the assistance and cooperation of all personnel, adequate security of TRAC-FLVN ADP facilities would be impossible.

3. Access. Access to the TRAC-FLVN's computer facilities and automated resources will be granted to TRAC-FLVN personnel, authorized contractor personnel, and other authorized users on an as-required basis. These facilities process classified information; therefore, entry is restricted. Personnel without security clearances, requiring access, must be authorized entry by the Chief, Computer Systems Division (CSD), Operations Directorate (OD), or the senior official controlling the facility and will be escorted at all times. Priority use of the systems will be given to TRAC-FLVN projects. Projects involving defense contractors must be coordinated with the C, CSD, during the development of the statement of work to ensure proper security controls are set forth and that adequate computer resources are available. The "no-one-alone rule," AR 380-380, paragraph 8-2a, should be adhered to whenever possible. However, due to the nature of TRAC's mission and operations, waivers have been granted to TRAC to allow personnel to work alone when needed.

a. A control zone will be established around each classified processing site in TRAC-FLVN. (Control zone is the area under control of the facility or area of computer operations.) Unescorted access to any part of a classified TRAC-FLVN data processing facility will be restricted to the personnel named on that facility's access roster.

(1) A facility access roster will be posted at the control-zone-entrance. Only personnel whose security clearance has been verified by the Security Division, DPTMSEC, CAC, need-to-know has been established, and an approved authorization for entrance has been granted by the ADPSSO, will be entrance has been granted by the ADPSSO, will be placed on this roster and have access to the computer room.

(2) Requests for access to a computer facility must be on a disposition form (DF) submitted to the C, CSD citing the individual's name, security clearance, and reason(s) that use of a particular facility is required. This DF will be signed by the immediate supervisor or, in the case of contractor personnel, by the contracting officer's representative (COR). Requests for access to a secure building will be coordinated with the security officer of the directorate responsible for that building.

(3) An access badge system is currently being used to control entry into certain facilities and buildings. Only those personnel outlined in (1) above will be issued an access badge by the Computer Systems Division. Access to multiple facilities in TRAC-FLVN will be based on authorized need and must be requested by the individual's supervisor as outlined in (2) above.

(4) Nongovernment personnel with an appropriate clearance and an established need-to-know will be authorized unescorted access into TRAC-FLVN's facilities but they will be required to sign into and out of the facility. The responsible TRAC-FLVN COR, or the official monitoring the contract which the nongovernment personnel are supporting, must request access to a facility by submitting a DF to the chief, Computer Systems Division, indicating the reason for access and certifying the need-to-know. The ADPSSO will provide an access badge to the nongovernment personnel only after the individual's security clearance has been verified by the Security Division, DPTMSEC. If no clearance is verified, a badge will not be issued and if entry is granted, the responsible official will designate an escort for the nongovernment personnel while using a facility. All nongovernment personnel, whether escorted or unescorted, will sign into and out of any TRAC-FLVN facility prior to and after each work session. In no case will nongovernment personnel be provided computer output (tapes, disks, or paper). Any such required output will be provided to the individual's government escort or sponsor by Computer Systems Division personnel. Once the output is given the appropriate government sponsor or escort, that person is responsible for ascertaining whether the information contained in the output is releasable to the contractor based on the security level of the information, the

contractor's right and need-to-know, and the sensitivity of the information (i.e., certain information is not releasable to nongovernment personnel or foreign personnel under any circumstances).

b. The following procedures apply to granting access to non-TRAC-FLVN military and DOD civilians, civilian contractors, and foreign nationals to TRAC-FLVN computer facilities

(1) Military and DOD civilian visitor clearances may be verified by checking the security clearance block of their official TDY order. Identity may be established by checking their military or civilian identification card. A need-to-know must be established before any classified information or material is released.

(2) Civilian contractors.

(a) Normal procedures are for visit requests to be forwarded-to-the Security Division, DPTMSEC, by the contractor or the contracting officer. (The official address is Commander, CAC & FL, ATTN: ATZL-GOP-SE, Fort Leavenworth, KS 66027-5070.) Visit requests serve to verify clearances and indicate classified information is required in connection with a specified contract or program. These requests are then forwarded to the Computer Systems Division by DPTMSEC. The ADPSSO will act on these requests.

(b) Unannounced visits of civilian contractors to a computer-facility will be reported to the ADPSSO before any information is released or access given to any facility or automated system. After the need-to-know is established and the visit is determined to be authorized, the ADPSSO will contact the Security Division, DPTMSEC, for assistance in verifying the individual's security clearance. It is the ADPSSO's responsibility to authorize access.

(c) Identity of visitors may be established by checking the contractor identification card. If the firm has no ID card, proof of identity may be made by checking a valid driver's license.

(3) Foreign nationals.

(a) Unannounced visits of foreign nationals must be reported to the ADPSSO before any information is discussed or access made to any facility or automated system.

(b) No foreign representative is authorized to make direct contact with this installation on official matters unless authorized by the Assistant Chief of Staff for Intelligence, Department of the Army (ACSI-DA). Foreign nationals or representatives who contact this installation without prior clearance from ACSI-DA will be instructed to contact their military attache in Washington, D.C.

(c) Locally-accredited foreign officers who desire visits to ADP facilities must make prior arrangements with the Deputy, TRAC, who will determine the visitor's accreditation. The Deputy, TRAC will subsequently approve or deny the visit.

c. Persons escorting visitors will ensure that classified materials are covered or locked in the safe, unless the visitor has an appropriate-level security clearance and a need-to-know.

d. Personnel requiring access to a TRAC-FLVN computer facility-during non duty hours (1630-0700 Monday through Friday, and Saturday, Sunday and holidays) may access a facility if their name is on the access roster and they are authorized to open and close the facility. If operations or system manager support is needed, coordination should be made with the appropriate personnel and should be provided at least a 24 hour notice.

4. Maintenance and cleaning personnel. The need-to-know principle precludes access to all ADP facilities. Therefore, any access provided to maintenance and cleaning personnel, even for that which is commonly referred to as "inadvertant access," would be unauthorized. These personnel, therefore, require an escort while in controlled or restricted areas.

5. Personnel security.

a. The ADPSSO is responsible for the conduct and mangement of the Personnel Security and Surety Program (PSSP) in accordance with AR 380-380, chapter 4. Coordination will be continuous with the CAC ADP systems security manager, AG, and CPO in the conduct of this program. A duty briefing for personnel entering ADP positions is at appendix F.

b. Personnel operating a system and controlling logical access (e.g., assigning passwords), or those who design, develop, install, modify, service, or maintain the security features of the operating system software, shall be cleared and have access authorization as appropriate for the highest classification and most restrictive category of material contained in the system. They shall be indoctrinated in the appropriate security procedures before assuming their duties.

c. Personnel requiring access to any part or component of the TRAC-FLVN ADP systems (and who could affect or modify the secure operations of the system or permit access to classified data or information) will have a security clearance and access authorization for the highest classification of material contained in the system. Maintenance personnel who need access to the system or controlled area will be accompanied by an escort designated for that purpose.

d. Certain restricted facilities and buildings require entry by means of an access badge. This badge is a controlled item and must be safeguarded and accounted for. A badge is issued to a particular customer, based on the individual's level of clearance, who needs to know/needs to use the information in the facility it provides access to. These badges will not be loaned or used by other individuals. They will not be displayed on uniforms or garments outside the facility or building they provide access to. In the event of loss, the ADPSSO will be immediately notified. The ADPSSO will periodically conduct random checks of access badges to support accountability and control. The ADPSSO will also conduct an annual changeover of cards and applicable access codes.

e. Directorates and staff organizations will develop procedures whereby personnel departing from their organization or leaving duties that are supported by the ADP systems are promptly identified to the ADPSSO and TASO. The ADPSSO and TASO will be responsible for deleting the departing individual's user ID and password from the system and they will transfer or delete the individual's files. The ADPSSO or responsible TASO (if applicable) will be contacted to effect these changes. Access badges to secure facilities will also be surrendered to the ADPSSO and removed from the appropriate access system. Physical access lock combinations, where applicable, will be changed to preclude future entry.

CHAPTER 2

PROCESSING SECURITY

Section I. Security Considerations

1. General. All personnel working within TRAC-FLVN ADP facilities, or using these facilities, should be familiar with the provisions of existing security regulations, especially AR 380-5 and AR 380-380. Conflicts between existing security regulations and this SOP will be reported to the TRAC-FLVN ADPSSO who should resolve them in favor of the existing security regulations. The TRAC-FLVN ADPSSO has responsibility for all security matters within HQ TRAC and TRAC-FLVN. The intent of this SOP is to allow processing of sensitive data in a secure ADP environment, with minimum impact on users, and to safeguard personnel and equipment from harm.

2. Access to ADPE. Access to ADP and office automation (OA) hardware must be strictly controlled and limited to authorized personnel only. Access to the hardware allows possible access to software and to data stored on the hardware; therefore, controlling access to hardware will also assist in controlling/protecting the data. Terminals accessing the hardware will be logged off at the completion of work or when left unattended. At the end of the workday, all terminals will be turned off, unless there is a technical reason for not doing so.

3. Privately owned computers. Privately owned computers are those computers which are not owned or leased by the government. Use of privately owned computers is strongly discouraged. When used, these computers must conform to the provisions of AR 380-380, paragraph 1-21. Privately owned computers will operate in a stand-alone mode only and will not process classified data. Any information processed and stored on these computers becomes the property of the U.S. Government. Use of privately owned computers must be approved by the TRAC-FLVN ADPSSO, with a memorandum of agreement (such as described at appendix G) executed between the owner and the TRAC-FLVN ADPSSO. Taking Government software and/or data home to work on a computer at home is prohibited.

Section II. Hardware Security

1. General. Hardware security includes the steps that must be taken to safeguard the equipment from physical damage and to safeguard the information processed from wrongful access. Future hardware security must be addressed in order to maintain a secure ADP environment.

2. Physical security. Physical security includes safeguarding ADP resources from physical damage or misuse, to the best possible extent. All personnel having access to ADP equipment must help maintain a secure environment by ensuring only authorized personnel are using the ADP equipment and by ensuring that the facility or area is secured when left unattended. At the end of the work day, all equipment should be powered off, unless there is a technical reason for not doing so and the area/building is secured. Risks to ADP equipment must be minimized to the extent feasibly possible and there should be a coordinated effort between physical security and ADP security personnel.

3. Processing security. All personnel must assist in maintaining processing security on all ADP equipment. For all ADP systems, this means protecting data from those who do not have a need to know and a valid clearance for that data. Passwords and/or read/write keys should be used to keep unauthorized personnel from accessing data.

4. Future considerations. AR 380-380 states, "Hardware security requirements must be considered in the future design, development, and acquisition of Army computer equipment." Hardware security must meet the needs of the data processed. As future data protection needs increase, hardware requirements for protecting the data will increase. Security features must provide for restricted access and, when possible/feasible, must restrict emanations from the equipment, or these features will have to be built into the facility housing the equipment. The required security features should be considered by appropriate individuals prior to procurement actions.

Section III. Software Security

1. General. Software security includes the steps necessary to safeguard operating systems and applications software from unauthorized access or exploitation. Future software security must be addressed in order to maintain a secure ADP processing environment.

2. Physical security. Physical security includes safeguarding operating systems software and applications software from physical damage, theft or misuse to the best possible extent. All personnel working with or having access to ADP equipment potentially has access to the software. System managers and the ADPSSOs are responsible to maintain all software in a secure environment. Spare copies of all software, if available, should be secured in GSA-approved safes for storage and safekeeping for backup purposes. Handling procedures for diskettes are at appendix H. Security procedures for data diskettes are at appendix I; security procedures for software diskettes are at appendix J.

3. Processing security. All personnel must assist in maintaining software processing security by using only those software packages authorized to be used. Access to software packages is limited to system managers and the ADPSSOs and then are only accessed to maintain system operations on a more secure processing environment. Users are authorized to use software packages in order to process programs and to perform routine tasks; but they are not authorized to make changes to these software packages.

4. Future considerations. Software must meet the security requirements of the data processed. As future data protection needs increase, security in software must improve to meet these needs. AR 380-380 states that "software security requirements must be considered in the future design, development, and acquisition of Army computer equipment." Security features must provide for restricted access and protection of data. Personnel in responsible positions must analyze the needs of the environment and consider the software packages that will best maintain a secure processing environment.

Section IV. Network Security

1. General. Networks provide the means for automation users to receive support on a remote computer system. The remote computer may be miles away or in the next room, yet it is capable of receiving input, processing the input, and providing output to remote terminals/sites. Maintaining control of the networks, who has authorized access to the networks, and what users are doing on the networks, is a must in order to achieve automation security. Networks linking remote facilities provide an increased opportunity for misuse/abuse or unauthorized access to computer systems/data and must therefore be secured to he the greatest extent possible for the level of data that may be accessed. Therefore, networks, whether classified or unclassified, must be afforded protection commensurate with the level of data they process/transmit.

2. Password security. Access to TRAC-FLVN VAX-based and INTEL-based computer systems is gained through a LOGIN procedure. The standard operating system has been modified to retain additional information required for security audit-trail purposes. The system will prompt the user to enter the required information. A unique user name and password will be issued to each user by the ADPSSO or alternate ADPSSO. They will be treated as secret information. The project assignment control number (ACN) will be supplied according to the project being worked on. A "U" or "S" will indicate unclassified or secret processing.

a. Each individual user will have a unique password assigned for-use at a remote terminal. The password is a group of characters assigned to each individual user by the ADPSSO/TASO. The password is required for the LOGIN procedure. For TRAC-FLVN VAX-based remote terminal users, the password is classified as secret and must be protected as such. It is the responsibility of the user to notify the ADPSSO/TASO whenever a password may have been compromised, i.e., inadvertently disclosured to unauthorized personnel.

b. When personnel no longer require system access, the password-to which they had access must be changed, and they should be removed from the system.

c. All passwords will be generated by random number generator software and all hard copies of passwords will be stored in a secure container under the control of the ADPSSO/TASO.

d. After individuals requiring access to a specific computer system are issued a password, the individual will not share this password even with persons with the same security clearance or working on the same application. Sharing passwords eliminates the password owner's protection against possible computer abuse for which he/she may be held responsible.

e. Individuals issued passwords will be required to acknowledge-reciept of password and to sign a statement of responsibility IAW AR 38Ø-38Ø, paragraph 5-3. A sample password receipt form is at appendix K.

3. Terminal security. The security requirements for any remote terminal and adjacent area will be as prescribed by Army regulations and the ADPSSO. All prescribed security measures must be implemented before any remote terminal may be connected to the TRAC-FLVN ADP systems or network, including OA equipment. The following considerations will apply to all remote terminal areas.

a. Access to terminals must be controlled and limited to authorized personnel. All terminals will be logged off upon completion of work. All terminals should also be powered off. Terminals utilized for processing of classified data are of special concern in this regard.

b. Each terminal site may implement policies as deemed necessary-to meet its unique needs by prescribing more detailed guidelines and instructions which are consistent with ARs 18-7, 38Ø-5, 38Ø-38Ø, and this SOP. This may be done in coordination between the responsible TASO and the ADPSSO. It is recommended that copies of remote-sites guidance and instructions be filed with this SOP. The application of these provisions will accomplish two objectives: 1) establishment of reasonable uniformity and 2) maintaining maximum security consistent with the assigned mission requirements.

c. Each site TASO is responsible for preparing and maintaining an operations SOP which contains a detailed set of procedures for equipment operations.

4. Comsec security. Encryption systems are installed to provide secure communications for classisfied networks. These systems are authorized to transmit information up to and including secret. Responsibilities for these facilities are outlined in the COMSEC security SOP, along with pertinent COMSEC emergency procedures.

5. LAN security. Local area networks (LAN) provide the means for access to various computer systems. These networks are capable of processing up to secret data and must be afforded appropriate protection. Access to LAN facilities must be limited to authorized personnel and/or those with a demonstrated need-to-know. Passwords will be afforded protection as outlined in paragraph 2 above. Compromise of passwords or unauthorized access to these networks should be reported immediately to the ADPSSO or other cognizant authority for the area.

Section V. Media Security

1. General. Various forms of media are used for input/output to TRAC-FLVN computer and OA systems. For purposes of this SOP, media librarian refers to those individuals who have control over and handle magnetic tapes/disks, whether they are operations personnel or users.

2. Magnetic media control.

a. General. The chief, Computer Systems Division (CSD), has overall responsibility for media library procedures. The peripheral equipment operator is responsible for implementing magnetic media library procedures and will serve as the media librarian. A Computer Operations Branch (COB) representative will maintain the media library at the Central Computer Facility (CCF) and the Wargaming Computer Facility (WCF).

b. Control.

(1) The media librarian will maintain an alphanumeric sequential file for each disk/tape within each computer facility. This tape/disk management system will consist of the following information as a minimum.

(a) Media identification (MID). The actual sequence number-assigned on specific tape/disk, with the first two positions reflecting an alpha representation of the device that the tape/disk was created on.

(b) User ID. User name and name of person(s) for which the media is being stored.

(c) Creation date. The actual data the information contained on magnetic media was generated.

(d) Label name. File identification for the data stored on media.

(e) Security classification code U, C, or S.

(2) A list of media will be provided to owners on a quarterly-basis for the purpose of eliminating media no longer required. Owners will circle the MID number of those volumes no longer required.

c. Media inventory.

(1) All media will be inventoried by a visual check prior to the close of business each day. All open slots in the storage racks will be accounted for by the librarian.

(2) Classified media in the computer facilities will be stored in an approved storage container, commensurate with classification of the data contained on the media.

(3) A physical inventory will be conducted at least every quarter with transactional updates. This will indicate the contents of the library and the physical location of each item.

d. Marking of magnetic media.

(1) Each type of magnetic media will have sequential MID numbers assigned . When a magnetic medium from an outside source enters one of TRAC-FLVN's computer facilities, it will have a CSD label containing the information in 2a(1) through (5) affixed. The MID number will remain permanently assigned if the media is to remain within one of TRAC-FLVN's computer facilities. If the original medium is to be returned to the originator, the original marking will be left attached and the TRAC-FLVN MID# removed prior to the time it is returned. When a piece of an unclassified medium from an outside source is to be used on a one-time basis for a period of less than one day, however, the media librarian will be informed that an outside medium is in the facility. A classified medium from an outside source will be brought under the control of the media librarian at the time it enters the responsible facility.

(2) Security classification labeling will be accomplished with one of the following labels as appropriate:

(a) DA Label 9Ø (secret).

(b) DA Label 91 (confidential).

(c) DA Label 1Ø1 (unclassified).

Media with a classification higher than secret are not authorized to be processed or stored at any of the ADP facilities within TRAC-FLVN.

(3) A TRAC-FLVN media-usage identification label attached to-each-piece of magnetic media. The information required on the label is self-explanatory and will be used to record the usage of that piece of media.

(4) Classified media which are temporary in nature (retained 9Ø days or less), or which change frequently, will be treated as "working papers." They will be marked with the highest classification of any information contained on the media and will be protected in accordance with the security classification assigned.

(5) User access to magnetic media will be strictly controlled-at-each facility. All media will be stored either in

the media library room or, if classified, in a media library safe. All users will have access to media through the librarian or other designated personnel. Only authorized personnel will remove or replace media in the library or safe. A user will request media by type and classification. If "blank media" is requested, a new user label will be filled out and attached to the medium at the time it is received from the librarian. This will ensure that information necessary for master file update is obtained by the librarian. Previously used media will be requested by MID number and label in order to ensure that the requestor is authorized to have access to the data. The librarian will verify that the label on the medium volume matches that specified by the requestor.

(6) A media control log will be maintained daily for each piece checked in or out of the library. It will contain the MID number, type of media, classification, person signed out to, time out, and time in. This log will be checked at the close of business each day to account for each piece removed from the library. If a facility is open after normal duty hours, the responsible person making the security check will be responsible for ensuring that the log is kept and that all media are accounted for prior to closing the facility.

(7) No media will be removed from TRAC-FLVN computer facilities-until the media librarian has been notified and appropriate release and transmittal documentation is prepared. DA Form 200 will be used to document all magnetic media. For classified media leaving a computer facility permanently, downgrading instructions will be obtained from the proponent organization and affixed to the media.

3. Printed media control. It is the individual user's responsibility to provide classification markings at the top and bottom of all pages of printed output which contain classified information. ADP-generated reports will be marked IAW AR 380-380, paragragh 8-11e. In addition, users are to become familiar with the utility print options (SPRT to print secret information, and UPRT to print unclassified reports), and will use the appropriate option when producing hard copy output on the VAX-based systems in one of TRAC-FLVN's computer facilities. All printed output from a hardcopy printer or tempested piece of OA equipment will also be appropriately marked and controlled by the user. Classified processing and output is not authorized on automated resources unless appropriate physical security, tempest, and accreditation measures have been met.

4. Working papers. Working papers are media which are temporary in nature (retained for 90 days or less) and stay within the confines and control of one of TRAC-FLVN's computer facilities where the media work is generated. These include tapes/disks which are updated at frequent intervals. Even though a tape or disk may contain data that would extend its retainability beyond

90 days, the data or information is frequently altered/changed and new "media" created at each update. Working papers containing sensitive information will be:

a. Dated when created and contain creator's name.

b. Marked with the highest classification of any information contained in the document and protected in accordance with the classification assigned.

c. Destroyed (degaussed) when they have served their purpose.

d. Accounted for and controlled in the same manner prescribed for a finished document of comparable classification when:

(1) Transferred to another computer facility or activity by other than electrical means. (For guidance in sending classified tapes or other media, see paragraph 2, Magnetic media control.)

(2) Released by the originator to an agency or activity outside TRAC-FLVN or when transmitted through message center channels within TRAC-FLVN.

(3) Placed permanently in a file system.

(4) Retained for more than 90 days from date of origin.

e. All media described above will be assigned downgrading or exemption instructions.

5. <u>Downgrading and declassification instructions.</u> All downgrading and declassification markings will be derivative in nature. All classified material processed will be accorded the highest overall classification of information or data contained therein as assigned by the appropriate agency. Users will mark all classified products of their processing IAW the instructions in chapter 8-12, AR 380-380.

CHAPTER 3

OTHER SECURITY CONCERNS

Section I. General

Security is everyone's responsibility. Suspected or actual security violations should be reported to the ADPSSO, assistant ADPSSO, or other cognizant authority immediately. It is not the user's responsibility to investigate security incidents; that is the duty of TRAC-FLVN security personnel, Fort Leavenworth Provost Marshal's Office, and the 902d Military Intelligence Group. Cooperation on the part of all parties involved is the key to accomplishing a successful investigation.

Section II. Access badges.

1. Purpose. These are plastic badges allow the bearer to gain access to one or more of TRAC-FLVN's classified computer facilities or controlled buildings. These badges are issued IAW guidelines set forth in this document to personnel who possess an adequate security clearance and a verified need-to-know. These badges are controlled items that are provided solely for the use of the individual to whom they are issued. They will be safeguarded at all times and will not be loaned or given to other personnel, regardless of circumstances. Loss of a badge constitutes a security incident.

2. Loss. In the event of loss, the responsible individual will report the facts and circumstances through his/her supervisor to the ADPSSO or TASO, as rapidly as possible for investigation. Initial contact should be followed by a DF to the ADPSSO, for for record, stating the circumstances around the lost badge.

3. Display. Access badges will not be visibly displayed on uniforms or garments outside the facility or building to which they provide access/entry.

4. Outprocessing. In the event of transfer from TRAC-FLVN, the individual will return the access badge to ADPSSO during outprocessing. Final clearance will not be granted until the badge is returned to the ADPSSO or COB. Personnel will also return their badges when their requirement for access to a facility or building is no longer necessary.

5. Inventory. Access badges will be inventoried annually by the TRAC-FLVN ADPSSO with assistance from the COB. Inventories may be conducted more often as deemed necessary by the Director, Operations Directorate or the TRAC-FLVN ADPSSO.

Section III. Emergency procedures

1. General. This section sets forth procedures for handling emergency situations that could occur at any TRAC-FLVN site. These procedures will be generalized and more specific procedures should be enforced at each facility.

2. Fire procedures.

a. Fire evacuation routes. Evacuation routes for each facility should be posted in a number of high-visibility locations within the facility. Through periodic fire drills, all personnel should learn the routes available to them.

b. Fire extinguishers. Hand-held fire extinguishers should be located throughout each facility. Signs should be posted in visible locations showing where fire extinguishers are located. At least one person should be assigned to each fire extinguisher to assist in extinguishing small fires and to minimize confusion during evacuation of the building.

c. Fires.

(1) Small fires. Every attempt possible should be made to extinguish a small fire which can easily be confined to a very small area such as a desk, a trash can, or a single piece of equipment. Electronic equipment in the area should be powered off to preclude any sudden explosion or larger electrical fire. If the fire cannot be confined or a large amount of smoke is being generated, call the fire department and evacuate the building.

(2) Large fires. In the event of a large fire which cannot be locally confined (e.g., to a desk, trash can or single piece of equipment, or dense smoke ensues), the fire department should be notified and all personnel should evacuate the building.

(3) Should a fire occur in a facility, both the main electrical breaker and the fire alarm switch must be thrown immediately. All personnel not assigned to fire extinguishers will evacuate the facility immediately. Personnel assigned to fire extinguishers should also evacuate if conditions exist which could cause serious injury, i.e., dense smoke or larger fire. Only CO2 (class B, C) fire extinguishers will be used within the computer facility. Water-type fire extinguishers will only be used outside the equipment area and on nonelectrical fires.

(4) Burning magnetic media (tapes/disks) produce highly toxic gases that could be fatal if inhaled. In cases where magnetic media are burning, evacuate the building immediately.

(5) Physical security personnel for each building are responsible to assign personnel to fire extinguishers. Coordination should be made with ADP security personnel for assignments in equipment areas.

(6) A Halon fire extinguishing system is installed in building 5ØW. This system will automatically dispense Halon 13Ø1 gas to extinguish a detected fire. While Halon 13Ø1 is harmless to humans in small quantities, the area should be evacuated until cleared by fire department personnel.

3. Evacuation procedures. If time permits, classified materials should be locked in safes or secured away from the fire within the building or removed and stored in an off-site location. All open/unlocked exits should be monitored by personnel to preclude access to other personnel except except firefighters, MPs, and other investigative personnel. Electrical power to the building should be shut off during the evacuation. Evacuate the building to a safe/reasonable distance, approximately 3Ø-5Ø yards or more if warranted by fire department or MP personnel or the intensity of the fire/smoke around the facility area.

4. Water/flood procedures. Water within a facility provides a means to inflict severe damage to automated equipment and could cause serious injury to humans under the right circumstances.

a. For facilities that have overhead sprinkler systems, plastic sheets should be available to cover automated equipment. If the sprinkler system should be activated, equipment should be powered off and covered with the plastic sheets. If the water cannot be turned off immediately, power to the building should be turned off and an evacuation made. Water shut-off valves should be identified and physical security personnel should assign personnel to be responsible for the valves.

b. Raised floor facilities. If water is detected/discovered under a raised floor area, every attempt to locate the source should be made. However, if the amount of water or the flow is excessive, electrical power should be shut off and, if possible, water to the facility should be turned off. The fire department should be contacted to assist in pumping water out of the facility, if necessary. Facility enginners or other responsible personnel should be contacted to assist in correcting the problem.

5. Bomb threat procedures.

a. These procedures are designed to alert personnel of actions required in the event of a bomb threat or an explosion.

b. When notification of a bomb threat or bombing is received, the individual receiving the call will immediately make the necessary notifications to ensure the safeguarding of life and property. The person receiving the threat will perform the following:

(1) Keep the caller on the line as long as possible. Attempt-to-contact the operator on another telephone in order to trace the call. Ask the caller to repeat the message. Record every word spoken by the person making the call. (See CAC & FL Form 719 for checklist, appendix L.)

(2) If the caller does not indicate the location of the bomb or the time of possible detonation, the person receiving the call should ask the caller to provide this information.

(3) Pay particular attention to any background noises such as voices, music, aircraft, traffic, etc.

(4) Listen closely to the voice (male or female) for details of quality, accents, and speech impediments.

(5) It is advisable to inform the caller that the building is occupied and the detonation of a bomb could result in a serious injury to many innocent people.

(6) Notify the Provost Marshal's Office (PMO) immediately, extension 2111. Then notify the TRAC executive officer (extension 4834). The senior responsible occupant of the building at the time the threat is received will determine whether or not to have the building evacuated.

c. When a bomb threat has been received, evaluated, and the decision to evacuate the building has been made, the following evacuation procedures should be executed:

(1) Notify personnel to evacuate the building. Evacuate in an orderly manner to prevent panic. Avoid use of the fire alarm system as a signal to evacuate; this may cause confusion.

(2) Do not change the physical state of electrical equipment; this may result in detonation if the explosive device has a radio/radar firing system.

(3) Evacuate a minimum distance of 100 yards from the building. Maintain eye contact with the building (especially all entrances) until the military police (MP) have arrived.

d. Search procedures should include the following

(1) A planned and orderly search will be conducted, utilizing volunteer personnel who are familiar with the area being searched and who can recognize items which are foreign to the daily routine.

(2) The building should be divided into sections with certain employees made responsible for the search of those areas. If the caller indicates the area in which the bomb is located, that area should receive immediate attention.

(3) Search personnel should be instructed not to alter the physical state of the area (i.e., turning on/off lights, plugging in/unplugging electrical appliances, etc.). If a suspicious object is found, notify MP personnel located on site. DO NOT DISTURB THE DEVICE IN ANY WAY.

(4) Search technique.

(a) Move to center of the area and listen for any peculiar sounds, primarily that of a clock-type mechanism.

(b) Begin search on outer limits of area/room and work toward the center.

(c) Mark area upon completion of search to preclude search by others.

e. Re-entry. Re-entry may be permitted only after a thorough search has been completed and when an appropriate time after the expected detonation has passed. The senior responsible occupant will authorize re-entry when danger from an explosion appears unlikely.

6. Terrorist group procedures. With the current world political situation, terrorist activities must be considered a possibility at Fort Leavenworth. These procedures are designed to alert computer personnel and users of actions required in the event of demands, threats, or actions by terrorist groups.

a. Demands.

(1) Report nature of the demand to your next available supervisor. The report will be passed from supervisor to supervisor until the commander is informed. The military police (extension 2111) will be notified as soon as possible by the person receiving the demand.

(2) If possible, the source of the demand, time, date, place, and circumstances of the receipt should be recorded in writing.

b. Threats. Same as paragraph a above.

c. Actions.

(1) Report nature of the action to your next available supervisor and to the Military Police (extension 2111). The report will be passed from supervisor to supervisor until the commander is informed.

(2) Determine, if possible, whether the action is overt (open to view, i.e., an open gathering of a dissident group), or covert (concealed operations, i.e., cutting of telephone lines).

(3) Record the time, date, place, and circumstances of the discovery of the actions.

7. Protection of classified material.

a. Emergency conditions may be categorized into three general types: natural disaster, enemy attack, and civil riot or uprising. Even though situations of this severity are highly unlikely at Fort Leavenworth, circumstances may arise where personnel in charge of secure installations can no longer control actions of extraneous personnel. Circumstances, such as severe tornados, fire, heavy personnel traffic caused by engineer construction activities, etc., must be anticipated. Protection of classified crypto key material, crypto equipment, and classified data must be provided by a systematic procedure that can be executed in a minimum length of time.

b. Classified storage containers located in the CCF and WCF areas are designated for use by the computer operations personnel only. The safe will store the crypto keys for the current month. These keys are classified secret and must be secured separately in the storage container within their own approved container. This container will only be opened when necessary and will be left open only long enough to remove materials for processing; otherwise, it will be closed and locked. Maintaining this container in a normal locked condition minimizes the possibility of compromise of stored classified materials, should emergency or chaotic conditions suddenly occur.

c. The cryptographic devices located in various TRAC-FLVN facilities are classified equipment. These are unclassified for external viewing, and will be keyed/zeroed daily as required to support the facility's operation. Once these devices are keyed, they will be safeguarded by appropriately cleared personnel during the workday. During periods of the day when these personnel are not available, the devices will be zeroed and the intrusion alarm system activated. If hostile conditions exist, the ADPSSO, assistant ADPSSO, or TASO/alternate TASO (as appropriate) will notify the Fort Leavenworth COMSEC custodian, Ms. Cindy Murphy at 2736, and describe existing conditions with an appraisal of possible risks to the encryption device. He/she will obtain appropriate follow-on instructions and advise the responsible personnel.

8. Secure telephone and facsimile.

a. A secure telephone unit (STU II) and secure facsimile have been installed in the teleconferencing facility (TCF) in building 52. There are telephone extensions in HQ, TRAC, the Technical Operations Directorate (TOD), and in COB connected by conduit. This equipment proovides secure communications with other similar equipment.

b. Calls made on the STU II will be logged in with Command Group, HQ TRAC. The STU II uses commercial phone lines which are external to the Fort Leavenworth system.

9. Essential elements of friendly information (EFFI).

a. EEFI is any information that may be of sensitive nature and of possible intelligence value. This does not mean that the information is classified or that it cannot be discussed. However, an individual should always stop to consider with whom one is dealing, under what circumstances, whether the information will be used for only official business purposes.

b. Sensitive information should not be discussed with others without determining their "need to know." Such information should not be passed to authorized personnel in an inappropriate environment (e.g., restaurant, club, etc.), nor should one provide more information on sensitive subjects than necessary.

c. EEFI pertinent to TRAC-FLVN include:

(1) Details of computer hardware and configuration.

(2) Remote processing sites and associated activities.

(3) Specific information about computer applications.

(4) Operating procedures.

(5) Specific safeguards of the TRAC computer systems, whether technical, physical, or procedural.

(6) Passwords.

(7) Information concerning scheduled VIPs and their itineraries.

1Ø. Summary. These emergency procedures are set forth to help protect the lives of personnel assigned to TRAC-FLVN, and to protect TRAC-FLVN automated resources to the best possible extent. These procedures are not all-encompassing and more stringent measures should be considered individually for each facility. It is the responsibility of the building's senior responsible personnel and the building's security personnel to develop and implement more effective measures at their own location.

APPENDIX A

GLOSSARY OF TERMS

1. Accreditation. The authorization and approval granted to a data processing activity or network to process classified or sensitive data. After certification by a competent authority, designated technical personnel verify that specified technical requirements for achieving adequate data security have been met.

2. Access. The ability and the means to approach, communicate with (input to and receive output from), or otherwise make use of any material or component in an ADP system.

3. Access category. One of the classes to which a user, a program, or a process in an ADP system may be assigned on the basis of the resource or groups of resources that each user, program, or process is authorized to use.

4. Access control. The process of limiting access to the resources of an ADP system only to authorized user, program, process, or other ADP systems (in computer networks). Synonymous with controlled access, controlled accessibility.

5. Access control mechanism. Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access to an ADP system.

6. Access list. A catalog of users, programs, or processes, and the specifications of access categories to which each is assigned.

7. Accountability. The quality or state which enables action or processes in systems to be traced to the individuals who performed them or caused them to happen.

8. ADP system. An assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention. ADP systems, defined here, the totality of automatic data processing equipment (ADPE) and include:

a. General and special purpose computers.

b. Commercially available components (those produced as a result of research and development) and the equivalent systems created from them regardless of size, capacity, or price, which are utilized in the creation, collection, storage, processing, communication, display, and dissemination of information.

c. Auxiliary for accessorial equipment, such as data communications terminals, source data automation recording equipment (e.g., optical character recognition equipment, magnetic tape cartridge typewriters, and other data acquisition devices) data output equipment (e.g., digital plotters and computer output microfilmers) to be used in support of digital, analog, or hybrid computer equipment, either cable-connected, or self-standing.

d. Electrical accounting machines (EAM) used in conjunction with or independently of digital, analog, or hybrid computers.

9. ADP system security. The hardware/software functions, characteristics, and features; operational procedures, accountability procedures and access controls at the central computer facility or remote computer terminal facilities; and the management constraints, physical structure, devices and personnel and communications controls needed to provide an acceptable level of protection in a computer system.

10. Arrest. The discovery of user activity not necessary to the normal processing of data which might lead to a violation of system security and force termination of the activity. Refers to ADP facilities, equipment, files, and the property of negotiables controlled or issued by ADP systems. The following specific definitions refer to the categories of assets used in the risk analysis.

a. Facilities. All building, air conditioning, furnishings, and other support equipment. Excludes any assets more properly classifiable in another asset category.

b. Equipment. All ADP equipment located in the continguous area known as the "computer facility." Does not include equipment that would <u>not</u> be lost in, say, a fire that completely destroyed the computer facility.

c. Software. All programs, documentation, and job control language (JCL) that would be lost in, say, a fire that completely destroyed the computer facility.

d. Files. All magnetic media data files that would be lost were the computer facility completely destroyed.

e. Data. An arbitrary value methodically applied to represent the proprietary value of all data maintained in the computer facility; any losses that might occur were the data compromised but not destroyed.

f. Negotiables. The value of all negotiable instruments produced on or by the computers operated in the computer facility or which might be fraudulently misappropriated, etc., by transactions entered into, created by, or otherwise processed in the computer(s) located in the computer facility (even though the eventual loss might be directly caused by another computer, another manual operation, or any combination of the two).

g. Materiel. The value of all tangible property controlled or accounted for by the computer(s) operated in the computer facility or which might be fraudulently misappropriated, etc., by transactions entered into, created by, or otherwise generated in the computer(s) located in the computer facility (even though the eventual loss might be directly caused by another computer, another manual operation, or any combination of the two).

h. Mission. The value of the operations and maintenance (O&M) budget of all activities using the computer facility, factored by the amount of the activity's workload that could not be performed without the computer (that is, the exchange value of all the functions dependent on the computer facility, reduced by the percentage of that dependency).

11. Audit. To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

12. Audit Trail. A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequency of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

13. Authentication.

a. The acts of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

b. A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

14. Authorization. The granting to a user, a program, or a process the right of access.

15. Automated security monitoring. The use of automated procedures to ensure that the security controls implemented within an ADP system are not circumvented.

16. Bounds checking. Testing of computer program results for access to storage outside its authorized limits. Synonymous with memory bounds checking.

17. Breach. The successful and repeatable defeat of security controls with or without an arrest which, if carried to consummation, could result in penetration of the system. Examples of breaches are:

a. Operation of user code in master code.

b. Unauthorized acquisition of ID password or file access passwords.

c. Access of a file without using prescribed operating system mechanisms.

18. Browsing. Searching through storage to locate or acquire information without necessarily being sought.

19. Call back. A procedure established for identifying a terminal dialing into a computer system by disconnecting the calling terminal and reestablishing the connection by the computer system's dialing the telephone number of the calling terminal.

2Ø. Caution statement. A statement affixed to computer outputs which states the highest classification being processed in an ADPS at the time the product was produced, and if data not requested by the user is contained therein, requiring its control at the level and its immediate return to the originating computer center.

21. Central computer facility. One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area even through they are connected to the Central Computer Facility by approved communication links.

22. Central processing unit (also mainframe). The central component or processor of the ADP system which contains the main storage, arithmetic, and logic functions, along with special registers and control panel.

23. Cipher system. A cryptographic system in which cryptography is applied to plain text elements of equal length.

24. Ciphertext. Unintelligible text or signals produced through the use of cipher systems.

25. Classified defense information. Official information which requires protection against unauthorized disclosure in the interests of the national security of the United States and which has been so designated in accordance with the provisions of Executive Order 11652: TOP SECRET, SECRET, CONFIDENTIAL.

26. Communications security (COMSEC). The protection that ensures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunications.

27. Compartmentalization.

a. The isolation of the operating system, user programs, and data files from one another in main storage in order to provide protection against unauthorized or concurrent access by other users or programs.

b. The breaking down of sensitive data into small, isolated blocks for the purpose of reducing risk to the data.

28. Compound. Includes all activities, agencies, commands, etc., within the boundary of an installation.

29. Compromise. An unauthorized disclosure or loss of sensitive defense information.

30. Compromising emanations. Unintentional data-related or intelligencebearing signals which, if intercepted and analyzed, disclose classified information being transmitted, received, handled, or otherwise processed by any information-processing equipment.

31. Computer network. A complex consisting of two or more interconnected computers.

32. Computer program. A list of logically sequenced instructions in machine sensible language which allow the computer to operate independently of human intervention while performing an operation of function supporting a data system application.

33. Confidentiality. A concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provided for such data about individuals as well as organizations.

34. Contained. Refers to a state of being within limits, as within system bounds, regardless of purpose or functions, and includes any state of storage, use, or processing.

35. Control zone. The space, expressed in feet or radius, that surrounds equipment that is used to process sensitive defense information and that is under sufficient physical and technical control to preclude an unauthorized entry or compromise.

36. Controlled mode. (See mode of operation.)

37. Countermeasure. That form of military science which by the employment of devices and techniques has as its objective the impairment of the operational effectiveness of enemy activity.

38. Crytographic system. The documents, devices, equipment, and associated techniques that are used as a unit to provide a single means of encryption (enciphering or encoding).

39. Data integrity. The state that exists when computerized data are the same as that in the source documents and have not been exposed to accidental or malicious alteration or destruction.

4Ø. Data processing installation. Any facility, room, or building housing ADP equipment and/or storage media. This term does not include the areas associated with the auxiliary power or output processing unless they are colocated with the DPI.

41. Data security. The protection of data from accidental, unauthorized, intentional, or malicious modification, destruction, or disclosure.

42. Dedicated mode. (See mode of operation.)

43. Degauss. Refer to appendix D for approved devices.

a. To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media, usually tapes. The process involves increasing the AC field gradually from zero to some maximum value and back to zero, which leaves an unreadable level of magnetization on the media.

b. Loosely, to erase.

44. Documentation. Records necessary for the orderly presentation, organization, and communication of specialized information (especially, records concerning the development, implementation, and maintenance of all relevant aspects of an ADP or data system).

45. Eavesdropping. The unauthorized interception of information bearing emanations through the use of methods other than wiretapping.

46. Electromagnetic emanations. Signals transmitted as radiation through the air and through conductors.

47. Emanations security (EMSEC). The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations.

48. Encryption.

a. End-to-end encryption. Encryption of information at the origin within a communications network and postponing decryption to the final destination point.

b. Link encryption. The application of online crypto operations to a link of a communications system so that all information passing over the link is encrypted.

49. Encryption algorithm. A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations to the normal representation of the information through the use of variable elements controlled by the application of a key.

50. Escort(s). Escort(s) are duly designated personnel who have appropriate clearances and access authorization for the sensitive or classified material contained in the system and are sufficiently knowledgeable to understand the security implications of and to control the activities and access of the individual being escorted.

51. Executive state. One of two generally possible states in which an ADP system may operate, and in which only certain privileged instructions may be executed; such privileged instructions may not be executed when the system is operating in the other (user) state. Synonymous with supervisor state.

52. Facility security profile. See AR 380-380.

53. Fail-safe. The automatic termination and protection of programs or other processing operations when a hardware or software failure is detected in an ADP system.

54. Fail-soft. The selective termination of affected nonessential processing when a hardware or software failure is detected in an ADP system.

55. File protection. The aggregate of all processes and procedures established in an ADP system and designed to inhibit unauthorized access, contamination, or elimination of a file.

56. "For official use only" (FOUO) information. That nonclassified official information of a sensitive, proprietary, or personally private nature which must be protected against unauthorized public release.

57. Handshaking procedurer. A dialogue between a user and a computer, a computer and another computer; a program for the purpose of identifying a user and authenticating his identity through a sequence of questions and answers based on information

either previously stored in the computer or supplied to the computer by the initiator of dialogue. Synonymous with password dialogue.

58. Hard copy. Printed copy of ADP output. Manipulable media, such as forms or cards, containing data records or processed information associated with ADP input/output.

59. Hardware. Physical equipment or devices of an ADP system; the computer and pheripheral equipment.

6Ø. Hardware security. Computer equipment features or devices used in an ADP system to preclude unauthorized access to data or system resources.

61. Identification. The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to an ADP system.

62. Individual accountability. Measures to positively associate the identity of a user with his access to machines, material, and the time, method, and degree of access.

63. Integrity. The capability of an ADP system to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

64. Intelligence. Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas, which is immediately or potentially significant to the development and execution of plans, policies, and operations.

65. Interactive computing. Use of a computer such that the user is in control and may enter data or make other demands on the system which responds by the immediate processing of user requests and returning appropriate replies to these requests.

66. Isolation. The containment of users and resources in an ADP system in such a way that users and processes are separate from one another as well as from the protection controls of the operating system.

67. Key. In cryptography, a sequence of symbols that controls the operations of encryption and decryption.

68. Loophole. An error of omission or oversight in software or hardware which permits circumventing the access control process.

69. Masquerading. An attempt to gain access to a system by posing as an authorized user.

70. Material. Data processed, stored, or used in, and information produced by, an ADP system regardless of form or medium (e.g., programs, reports, data sets or files, records, and data elements).

71. Memory bounds. The limits in the range of storage addresses for a protected region in memory.

72. Mode of operation. The security environment and method of operating and ADP system. There are three modes of operation:

a. Dedicated. The use and control of a central computer facility, its connected peripheral devices, and remote terminals exclusively by specific users or groups of users for the processing of a particular type(s) and category(ies) of sensitive defense material. All users of the system are cleared and have access authorization for all material in the ADP system. All storage media are either purged or removed from the computer and, together with other output, safeguarded as appropriate to its classification or sensitivity before resuming processing in a less restrictive mode.

b. Controlled. Reliance is placed upon various security controls and countermeasures to permit operation of an ADP system in a mode of operation which is less restrictive than dedicated and more restrictive than multilevel. Examples are:

(1) Compartment. Utilization of a resource-sharing computer system for the concurrent processing or storage.

(a) Of two or more types of sensitive compartmented information or

(b) Of any type of sensitive compartmented information with some other kind of information. System access is afforded personnel holding top secret clearances, but not necessarily all the sensitive comparted information access approvals involved. Storage areas containing compartment information are purged before continuing processing and outputs may require special handling.

(2) System high or benign environment. Information of different levels of classification or special category designations are processed simultaneously in the same computer system while procedural and physical security controls commensurate with those prescribed for the highest classification being processed. In this mode, all data processed, along with any outputs generated, will be considered to be of the same classification/category as the highest level being processed until determined otherwise. (See default classification.) All

users are cleared for the highest level, but not necessarily having a need-to-know for all data, and reliance is placed on the ADPS for routing and need-to-know separation of data.

c. Multilevel security mode. A mode of operation using an operating system (supervisor or executive program) which provides a capability that permits various levels and categories or compartments of material to be concurrently stored and processed in an ADP system. In a remotely accessed resources sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accommodate the concurrent processing and storage of:

(1) Two or more levels of classified data.

(2) One or more levels of classified data with unclassified data depending upon the constraints placed on the systems.

73. Multilevel security mode. See mode of operation.

74. Multiple access rights terminal. A terminal that may be used by more than one class of users; for example, users with different access rights to data.

75. Need-to-know. The necessity for access to knowledge of, or possession of, classified or other sensitive defense information in order to carry out official military or other governmental duties. Responsibility for determining whether a person's duties require that he possess or have access to certain information, and whether he is authorized to receive it, rests upon the individual having current possession, knowledge, or control of the information involved. This is not the responsibility of the prospective recipient.

76. Off-line. Operation of the peripheral equipment of an ADP system without automatic control by the central processing unit.

77. On-line. Operation of components of an ADP system, including peripheral equipment, under direct control of the central processing unit, by which information reflecting current activity is introduced into the ADP system, or output from the ADP system as soon as it occurs directly in sequence with the main flow of data processing.

78. Operating system (O/S). An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform debugging, input-output, accounting, resource allocation, compilation, storage assignment tasks, and other

system related functions (synonymous with monitor, executive, control program, and supervisor).

79. Operational data security. The protection of data from either accidental or unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations.

8Ø. Output. Information or data transferred from the internal storage of a computer to secondary or external storage, or to any device outside of the computer; also, the process of such data transfer.

81. Overwriting. The obliteration of recorded data by recording different data on the same medium.

82. Password. A protected word or a string of characters that identifies or authenticates a user, a specific resource, or an access type.

83. Password dialogue. Synonym for handshaking procedure.

84. Penetration. A successful unauthorized access to an ADP system.

85. Periods processing. Periods of time during which various levels of security classifications are processed at different times with the system being purged between periods.

86. Peripheral device or equipment. Auxiliary devices which may be placed under the control of the central computer, whether for on-line or off-line operations.

87. Personnel security. The procedures established to ensure that all personnel who have access as well as all appropriate clearances.

88. Physical control zone (PCZ). The space surrounding equipment processing sensitive defense information, which is under sufficient physical and technical control to preclude a successful hostile intercept of any such information from within this space.

89. Physical security.

a. The use of locks, guards, badges, and similar measures to control access to the computer and related equipment.

b. The measures required for the protection of the structures housing the computer, related equipment, and their contents from damage by accident, fire, and environmental hazards.

90. Piggyback entry. Unauthorized access that is gained to an ADP system via another user's legitimate connection.

91. Plain text. Intelligible text or signals that have meaning and that can be read or acted upon without the application of any decryption.

92. Principle of least privilege. The granting of the minimum access authorization necessary for the performance of required tasks.

93. Print suppress. To eliminate the printing of characters in order to preserve their secrecy; for example, the characters of a password as it is keyed by a user at an input terminal.

94. Privacy.

a. The right of an individual to self-determination as to the degree to which the individual is willing to share with others information about himself that may be compromised by unauthorized exchange of such information among other individuals or organizations.

b. The right of individuals and organizations to control the collection, storage, and dissemination of their information or information about themselves.

95. Privileged instructions. The management constraints; operational, administrative and accountability procedures; and supplemental controls established to provide an acceptable level of protection for sensitive defense information and data.

96. Profiles. An accurate and detailed security description of the physical structure; equipment components, their locations and relationships, and general operating environment within which the ADP system operates.

97. Protected wireline distribution system (PWDS). A telecommunications system which has been approved by a legally designated authority and to which electromagnetic and physical safeguards have been applied to permit safe electrical transmission of unencrypted sensitive information.

98. Protection ring. One of a hierarchy of privileged modes of an ADP system that gives certain access rights to programs and processes authorized to operate in a given mode.

99. Purging.

a. The orderly review of storage and removal of inactive or obsolete data files.

b. The removal of obsolete data by erasure, by overwriting of storage, or by resetting registers.

100. Recovery procedures. The actions necessary to restore a system's computational capability and data files after a system failure or penetration.

101. Red/black concept. The concept that electrical and electronic circuits, components, equipment, systems, and so forth, which handle classified plain language information in electric signal form (red) be separated from those which handle encrypted or unclassified information (black). Under this concept, red/black terminology is used to clarify specific criteria relating to, and to differentiate between such circuits, components, equipment, systems, etc., and the areas in which they are contained.

102. Reliability. The generic ability to a given ADP system to satisfactorily perform the assigned mission for a given time interval when used under stated conditions.

103. Remanence. The residual magnetism that remains on magnetic storage media after degaussing.

104. Remote terminal area. Remote computer facilities, peripheral devices, or terminals which are located outside the central computer facility.

105. Remotely accessed resource-sharing computer system. A computer system which includes one or more central processing units, peripheral devices, remote terminals, and communications equipment or interconnection links, which allocates its resources to one or more users, and which can be entered from terminals located outside the central computer facility.

106. Residue. Data left in storage after processing operations and before degaussing or rewriting has taken place.

107. Resource. In an ADP system, any function, device, or data collection that may be allocated to users or programs.

108. Resource sharing. In an ADP system, the concurrent use of a resource by more than one user, job, or program.

109. Resource-sharing computer system. A computer system which uses its resources, including input/output (I/O) devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities, to enable one or more users to manipulate data and process coresident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as time-sharing, multiprogramming, multiaccessing, multiprocessing, or concurrent processing.

11Ø. Risk. The total dollar amount of loss that may be expected from the action of a given threat against a specific asset. Usually expressed in annual amounts and called by some "annual loss expectancy" (ALE).

111. Risk analysis. An analysis of system assets and vulnerabilities to establish an estimate of risk based on estimated probabilities of occurrence and predicted impact of given threats against the totality of ADP assets.

112. Risk management. An element of managerial science concerned with the identification, measurement, control, and minimization of uncertain events. An effective risk management program encompasses the following four phases: (1) risk analysis; (2) management decision; (3) control implementation; and (4) effectiveness review.

113. Safeguard statement. A statement affixed to computer outputs which states the highest classification being processed in an ADPS at the time the product was produced and requiring its control at that level until a responsible person can determine its true classification.

114. Secure configuration management. The sum of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that such changes will not lead to a decreased data security.

115. Secure operating system. An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and resources managed by the operating system.

116. Secure working area. An accredited facility which is used daily for handling, discussing, or processing of sensitive defense information.

117. Security incident. Any incident involving classified or sensitive information in which there is a deviation from the requirements of governing security regulations (compromise, inadvertent disclosure, need-to-know violations, fraud, and administrative deviation are examples of a security incident).

118. Security test and evaluation (ST&E). An examination and analysis of the security features of an ADP system as they have been applied in an operational environment to develop factual evidence upon which a certification can be based.

119. ST&E tools and equipment. Specialized techniques, procedures, criteria, standards, programs, or equipment accepted by qualified security testing and evaluating (ST&E) personnel for uniform or standard use in testing and evaluating secure features of ADP systems.

120. Sensitive compartmented information (SCI). Includes only that intelligence material having special controls indicating restrictive handling for which systems of compartmentation or handling are formally established (DoD 5200.1-R).

121. Sensitive information. Any information which requires a degree of protection and which should not be made generally available. This type of information includes, but is not limited to, that information which must be safeguarded so as to:

a. Prevent damage to the national defense and which usually bears a security classification.

b. Assure the individual privacy of US citizens as provided by the Privacy Act of 1974.

c. Maintain the confidentiality of for official use only information derived from inspector general, auditory, or other investigative activities such as medical or jurisprudence/disciplinary information derived from records of doctor/patient or lawyer/client relationships.

d. Protect funds, supplies, and material from theft, fraud, misappropriation, or misuse. This includes asset/resource accounting or authorizing systems or operations which are involved in the control and distribution of funds or the processing of information which offers the opportunity to divert economically valuable resources, e.g., supplies, dollars, or data.

e. Protect proprietary information which is the exclusive property of a civilian corporation on loan from industry to government or made available to government for its proper use in evaluating or adjudicating contracts.

f. Protect government-developed privileged information involving the award of contracts.

122. Software. The totality of programs, routines, and documentation utilizing or describing the capabilities of computers and data systems.

123. Software security. Those general purpose (executive, utility, or software development tools) and applications programs, and routines which protect data or information handled by an ADP system and its resources.

124. Storage (also memory). Component or device in which data can be sorted and/or retrieved by a computer.

a. Auxiliary storage. Storage device used in addition to the main storage of a computer (e.g., magnetic tape, disk, or drum) which usually has a much larger capacity for data but which is slower to access.

b. Main storage. Usually the fastest device used in/by a computer for the storage of data, and the one from which instructions are executed.

125. System integrity. The state that exists when there is complete assurance that under all conditions an ADP system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and data integrity.

126. Telecommunications. Any transmission, emission, or reception of signs, signals, writing, images, sounds, or other information by wire, radio, visual, or any electromagnetic systems.

127. Teleprocessing. Pertaining to an information transmission system that combines telecommunications, ADP systems, and man-machine interface equipment for the purpose of interacting and functioning as an integrated whole.

128. Teleprocessing security. The protection that results from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure, acquisition, manipulation, or modification of information in a teleprocessing system.

129. Terminal identification. The means used to establish the unique identification of a terminal by an ADP system.

130. Threat. Any undesirable thing that might happen to an ADP facility or system. For purposes of risk analysis of facilities (see chapter 3), threats have been arranged into 17 categories, defined as follows:

a. Fire. Refers to all forms of fire regardless of origin.

b. Flood. All water-caused damage, whether from rain, rising tides, broken pipes, or discharged sprinkler systems. "Flood" excludes accidental or purposeful spilling of water onto ADP equipment by personnel.

c. Windstorm. Includes physical damage caused directly by high winds, hurricanes, tornadoes, and thunderstorms (but not rain).

d. Earthquake Self-explanatory.

e. Human error. Comprised of all categories of careless, accidental, non-purposeful damage or disruption directly or indirectly caused by human action.

f. Power failure. Describes any loss of electrical power that causes disruption of computer operations.

g. Air conditioning failure. Self-explanatory. (Does not include power failures.)

h. Communications failure. Any disruption or compromise caused by the failure of communications lines or links to perform in the manner expected.

i. Hardware failure. Any disruption or compromise caused by the failure of ADP equipment to perform its designed function.

j. Unauthorized access. Any loss or compromise directly traceable to the penetration of the facility or of the systems operated in the facility by unauthorized persons or for unauthorized purposes.

k. Unauthorized use. When a user is authorized to access a system but uses the system for a purpose other than performance of job-related tasks.

l. Sabotage I. The willful destruction or disruption of ADP assets by an employee of the ADP facility.

m. Sabotage II. The same kind of act committed by an employee not connected with the ADP operation.

n. Sabotage III. The same but by a person not employeed by the facility.

o. Fraud I. Identifies any theft, misappropriation, embezzlement, falsification, or criminal misuse of data stored and/or processed by computers. The perpetrator is an ADP employee.

p. Fraud II. Same act committed by an employee not connected with ADP.

q. Fraud III. Same act committed by a person not employed by the facility.

131. Time-dependent password. A password which is valid only at a certain time of the day or during a specified interval of time.

132. Traffic flow security. The protection that results from those features in some crypto equipment that conceal the presence of valid messages on a communications circuit, usually by causing the circuit to appear busy at all times, or by encrypting the source and destination addresses of valid messages.

133. Trap door. A condition existing in the system software or hardware which can be triggered to subvert the software or hardware security features. Basically there are two kinds of trap doors: First, the condition is triggered by something internal to the system (e.g., a counter, a date/time value or any

specific set of preestablished circumstances); second, a condition is triggered by an external input to the system (e.g., a remote terminal or application program input message).

134. Trojan horse. A computer program that is apparently or actually useful and that contains a trap door.

135. User (customer). Any authorized person, office, or staff agency who may directly use or receive services or products from the computer system.

136. Validation. That portion of the development of specialized ST&E procedures, tools, and equipment needed to establish acceptance for joint usage by one or more DoD components or their contractors. Such action will include, as necessary, final development, valuation, and testing leading to acceptance by senior ST&E staff specialists of the three military departments or a defense agency, and approval for joint usage by the appropriate DoD authority.

137. Verification. The successful testing and documentation of actual online system penetration or attempts to penetrate the system in support or in contradiction of assumptions developed during system review and analysis which are to be included in the evaluation report.

138. Vulnerability. Any weakness or flaw existing in an automated system.

139. Vulnerability assessment. A measurement of:

a. The susceptibility of a particular system to a specific attack.

b. The opportunity available to a threat agent to mount that attack. A vulnerability is always demonstrable but may exist independently of a known threat. In general, a description of a vulnerability taxes account of those factors under friendly control.

140. Wiretapping.

a. Active. The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining access to data through the generation of false messages or control signals, or by altering the communications of legitimate users.

b. Passive. The monitoring and/or recording of data while the data is being transmitted over a communication link.

APPENDIX B

ADPSSO DUTIES

1. Implementing and enforcing security directives and procedures applicable to ADP operations and the use of automated equipment resources.

2. Initiating security planning for the projected classified use of ADP resources.

3. Acting as liaison with the installation security officer (ISO), installation automation system security manager (SSM), communications electronics manager, and signal security personnel in the 902d Military Intelligence Group.

4. Formulating and integrating proper security controls into the TRAC-FLVN ADP security SOP (this document).

5. Conducting sensitivity and risk analyses for new computer facilities and/or new automated equipment prior to their use. Preparing and submitting facility security profiles and accreditation requests for automated systems.

6. Requesting the conduct of an ADP security survey by CAC or 902d MI Group security specialists prior to the installation of new equipment, whose intended use is for classified processing; and coordinating requests for the conduct of security inspections of ADP facilities when the ADP system configuration is modified.

7. Conducting semiannual security and hazards indoctrination, briefings, and training for personnel who operate and use the TRAC-FLVN automated resources.

8. Maintaining surveillance over the hardware and software configuration safeguards, with the support of assistant ADPSSOs and terminal area security officers (TASOs).

9. Conducting periodic tests to assure that access limitations applicable to the various automated resources and facilities are adequate and effective.

10. Reporting promptly to the chief, Information Management Office, any system weakness/failure that could lead to the unauthorized disclosure of classified or otherwise sensitive information.

11. Preparation and submission of annual or biennial accreditation review documentation for designated TRAC-FLVN systems and facilities. The frequency of the accreditation review process is based on the sensitivity of the information processed, the changes made to the particular system, the threats to the system, or the system's vulnerabilities. Significant

changes to any of this should result in a more frequent review of the accreditation action for the affected system.

12. Supervising and coordinating all aspects of hazard protection (to include those associated with systems security).

13. Performing random monitoring of mass storage media contents to ensure compliance with file handling and security procedures by users.

14. Advise and assist the assistant ADPSSOs in the development of continuity of operations plans (COOP).

15. Ensure that application software is reported according to AR 18-22.

16. Control and manage the generation and issuance of system passwords.

17. Ensure that all involved with the procurement of hardware, software or systems services for ADPE and OA equipment are aware of the firm requirement to comply with automation security, as specified in paragraph 1-5h(3), AR 380-380.

18. Ensure that a TASO is properly appointed in writing for each terminal, group of continguous terminals, or OA equipment.

19. Cause operations to be partially or completely suspended upon detection of any action which may affect the security of the operation.

20. Immediately investigate and bring to the attention of the chief, Information Management Office, any known or suspected security incident or violation.

21. Implement and control the organization's personnel security and surety program as outlined in chapter 4, AR 380-380.

22. Control and provide systems security for the Digital VAX computers, standalone computers, the TRAC-FLVN computer network, graphic equipment, and supporting equipment in the Central Computer Facility and Teleconferencing Facility, both located in building 52.

23. Serving as the central point of contact for those assigned ADP security responsibilities within and without the organization in order to resolve questions and problems related to system security.

24. Conducting attempts to penetrate the security measures, methods, and features which use or may be established to protect the integrity of information in the ADP system in order to verify or deny the adequacy of hardware, software, and administrative procedures involved.

25. Ensuring that personnel who install, operate, maintain, use, and manage ADP and/or word processing systems are trained in security requirements and responsibilities.

APPENDIX C

ASSISTANT ADPSSO DUTIES

The assistant ADPSSO appointed for each TRAC ADP system will:

1. Advise the ADPSSO upon detection of any action which may affect the security of operations.

2. Ensure implementation of automation security regulations by:

a. Assisting the ADPSSO in preparing/maintaining the TRAC automantion security SOP.

b. Assisting the ADPSSO in conducting periodic surveys to determine compliance with the TRAC SOP and AR 380-380.

c. Maintaining continual awareness of threats and vulnerabilities so as to advise the ADPSSO of needed actions to minimize risks.

3. Report immediately to the ADPSSO any attempt to gain unauthorized access to sensitive defense information or any system failure or suspected defect which could lead to unauthorized disclosure.

4. Ensure that a TASO is properly appointed in writing for each terminal or group of contiguous terminals connected to the system.

5. Brief new users on system-specific ADP security policies, procedures, and requirements.

6. Issue and control physical access authorization of personnel with a demonstrated requirement to access the system (including users, contractors, and maintenance personnel).

7. Assist the ADPSSO in compiling and maintaining the facility security profile.

8. Control and manage the generation and issuance of system passwords.

9. Audit/review on a periodic basis files within the system to determine appropriateness/legality of file contents.

10. Assist the ADPSSO in compiling accreditation documentation to accompany TRAC's request for accreditation from commander, CAC.

11. Develop a continuity of operations plan (COOP) in coordination with the ADPSSO, for the system(s) he/she is responsible for.

APPENDIX D

TASO RESPONSIBILITIES

1. Scheduling and controlling personnel access to remote terminals, when necessary. Ensuring that instructions specifying security requirements and operating procedures for each terminal area are issued to the using personnel.

2. Initiating timely actions to stop terminal processing and implementing corrective measures if security deficiencies are discovered in his/her area of responsibility or within the TRAC-FLVN network.

3. Managing the control and dissemination of user name/passwords (UN/PW), that are provided by the ADPSSO. In addition, the TASO will investigate any possible security violation caused by the misuse of UN/PW.

4. Accounting for the equipment in his/her terminal area that is hand-receipted from the Computer Systems Division.

5. Ensuring that each user's identity, need-to-know, level of clearance, and access authorization are established prior to issuing a user name/password; supporting the use of the equipment or system.

6. Implementing controls to prevent entry of unauthorized transactions or data (e.g., classified data over unsecured data transmission lines) through user access terminals.

7. Assist the ADPSSO in providing system security.

8. As soon as possible, report to the ADPSSO all practices dangerous to system security and all security violations.

9. Support the ADPSSO in the implementation, control, and monitoring of the personnel security and surety program outlined in chapter 4, AR 380-380.

APPENDIX E

NETWORK SECURITY OFFICER DUTIES

The network security officer (NSO) appointed for each network processing sensitive defense information will:

1. Ensure that standard automation security procedures and protocols governing network operations are developed and promulgated.

2. Ensure that measures and procedures used at network modes fully support the security integrity of the network and comply with applicable command, DA, and DOD security directives.

3. Control access and connectivity to the network (that is, access to a node in the network other than the local node to which the user is logged in).

4. Function as the single point of contact for all aspects of network automation security.

5. Cause operations to be suspended, partially or completely, upon detection of actions which may affect the security of the network. Suspend any user not adhering to official regulations and procedures.

6. Ensure implementation of applicable automation security regulations by:

a. Preparing, disseminating, and maintaining plans, instructions, guidance, and SOPs concerning security of the network.

b. Conducting periodic surveys or reviews to determine compliance with such regulations.

c. Conducting reviews of threats to and vulnerabilities in the network.

7. Report immediately to the network manager any system failure which could lead to the unauthorized disclosure or attempts to gain unauthorized access to sensitive defense information.

8. Take measures to protect network assets from damage, destruction, alteration, or misappropriation.

9. Review and evaluate the security impact of changes to the network, including interfaces with other networks.

1Ø. Advise the network manager of available US Army Intelligence and Security Command (INSCOM) computer security services.

11. Ensure that audit trails and other system management reports are reviewed daily and used for internal security audits or testing.

12. Compile and maintain the network security profile.

APPENDIX F

DUTY BRIEFING FOR ADP SENSITIVE PERSONNEL

1. You have been assigned duties involving the use of a computer system that processes sensitive defense information. Army data processing activities (DPAs) are designated as critically sensitive, highly sensitive, sensitive, or nonsensitive according to the criteria given in paragraph 1-8 of AR 380-380, as follows:

a. Critically sensitive includes classified defense information or information involving large dollar volumes of asset/resource accounting or authorization data ($25 million per annum or higher).

b. Highly sensitive information is information not included in the above but including Privacy Act data and/or asset/resource accounting or authorization data of moderate dollar value ($1 million to $25 million).

c. Sensitive information is information not included in the above that includes lower dollar value asset/resource, proprietary, or contractual information.

d. Nonsensitive information not included in a, b, or c above.

2. Your job is designated as ADP sensitive because of the level(s)/variety/ volume of information you can access or because your job category is considered sensitive by regulation. Since your job is designated as ADP sensitive, you and your supervisor are being informed of this fact and you are being included in the ADP personnel security and surety program (PSSP) for this activity. This PSSP program is based on paragraph 1-10 and on chapter 4 of AR 380-380.

3. Screening for personnel in the PSSP is more extensive than the routine screening and clearance for personnel without this rating. In addition, personnel in ADP sensitive positions are subject to a continuing check by supervisors and are required to participate in continuing ADP security education, according to paragraph 4-9 of AR 380-380. The "surety" aspect of the program refers to this security maintenance concept. The continuing education required is shown below and is oriented toward your job duties and responsibilities.

a. All ADP sensitive personnel.

(1) Read required material in the regulations.

(2) Attend briefings.

b. Computer room personnel.

(1) Training in "a" above.

(2) Hazard training.

(3) Training for emergency shut-down procedures.

(4) Periodic reading of SOPs are required by computer center management.

c. Systems programmers.

(1) Training in "a" above.

(2) Training in procedures for protecting sensitive and above information.

4. Your job assignments require your receipt of a user ID and password that permit access to a computer system processing sensitive information. You must bear in mind that paragraph 5-3 of AR 380-380 requires all such passwords to be controlled at least at the highest level of sensitive information in the system.

5. I am required to impress upon you the extreme need for caution and discretion in any contacts either personal or professional. As in any interesting activity, the temptation is great to refer to your professional accomplishments. You are cautioned to avoid any conversation that could result in a disclosure of sensitive information to unauthorized personnel.

I have been briefed on the above and understand my responsibilities.

NAME (Printed)

DATE

SIGNATURE

ADPSSO/AADPSSO/TASO/OTHER

LAB/BRANCH/OFFICE/SECTION

SIGNATURE

APPENDIX G

AUTOMATION SECURITY AGREEMENT

An Agreement Between ______________________________________ and the US Army.
(Name - Printed or Typed)

1. Purpose. To obtain individual agreement to abide by established automation security requirements and procedures.

2. References:

a. AR 380-380, Automation Security

b. AR 380-5, Department of the Army Information Security Program

c. AR 340-17, Release of Information and Records from Army Files

d. AR 340-21, The Army Privacy Program

e. AR 600-50, Standards of Conduct

3. Problem. Automated (computer) systems have become an integral and essential part of Army operations. Protection of these systems and the information processed on them is of crucial importance. Each user of such systems must be fully aware of his/her responsibilities and agree to protect all aspects of automated systems.

4. Scope. This memorandum outlines general responsibilities of both the Army and the individual user of Army automated systems. Signature by both the individual and the Army representative indicates understanding of, and agreement to abide by, not only these general responsibilities but also the specific requirements stated in references.

5. Understandings and agreements.

a. All classified and sensitive information, regardless of format (paper document, magnetic storage, electronic signals, etc.), must be protected in accordance with references 2b through 2e above.

b. Army automated systems are to be used only by authorized personnel and only for officially approved purposes.

c. Automated systems must be protected according to reference 2a above, as well as command, installation, and activity security procedures. Such protective measures include, but are not limited to, the following:

(1) Systems will not be left in an operational mode (i.e. "signed on") while unattended.

(2) Passwords providing access to automated systems will be individual (not shared with others or publicly posted) and will be protected to the same degree as the information to which they give access.

(3) Suspected or actual security incidents, both potential and existing, must be reported immediately to security personnel.

d. Should the undersigned user of Army automated systems also privately own computer equipment which he/she wishes to use to perform official business (such use is strongly discouraged), the following shall apply:

(1) Privately-owned computer equipment must comply with all provisions of reference 2a, including accreditation. The equipment must be registered with the activity automation security point of contact. These actions must be completed prior to using the equipment for official business.

(2) Privately-owned equipment will not be used to process classified information.

(3) Privately-owned equipment may be used only in a stand-alone configuration. Privately-owned equipment may not be used to access a government-owned computer system.

(4) All information processed on a privately-owned system in support of official business becomes property of the U.S. Army.

(5) The owner of privately-owned equipment waives all rights to claim compensation for such use of the equipment.

(6) The government will not be responsible for loss, theft, destruction, damage, or wear and tear of privately-owned equipment.

6. Effective Date. This agreement becomes effective when it is signed and dated.

SIGNATURE	DATE

ORGANIZATION

SIGNATURE OF ARMY REPRESENTATIVE	TITLE	DATE

CAC&FL Form 1-65
1 Mar 87

APPENDIX H

PROTECTION PROCEDURES
COMMERCIAL SOFTWARE AND DATA DISKETTES

Diskettes must be protected when removed from their protective jackets. Therefore:

1. Do not place diskettes on terminals, in books, or under equipment. Do not toss a diskette loosely in a drawer.

2. Avoid placing diskettes near any magnetic source such as telephones, radios, tape recorders, or speakers of any kind.

3. Diskettes scratch easily. Do not touch exposed areas or try to wipe them clean.

4. Keep diskettes out of direct sunlight and away from extreme heat or cold.

5. Do not bend diskettes or place rubberbands or paper clips on them.

6. Do not write directly on a diskette with a ballpoint pen, lead pencil, or other hard writing instrument. Instead use a felt-tip pen and a label.

7. Diskettes should be stored vertically in their jackets in either diskette storage trays or boxes to avoid pressure to the sides.

8. Diskettes containing sensitive information should not be left unattended in personal computers or word processors.

9. Diskettes should not be exposed to unnecessary pollution such as cigarette ashes or smoke, liquids, or foods of any kind.

APPENDIX I

SECURITY PROCEDURES
DATA DISKETTES

1. Diskettes containing sensitive Privacy Act data will be marked "FOR OFFICIAL USE ONLY - Privacy Act Data." Both the label on the diskette and its protective jacket will be appropriately marked.

2. Diskettes containing classified data will be handled and marked IAW AR 380-5 (DA Information Security Program). Both the label on the diskette and its protective jacket will be appropriately marked.

3. Diskettes will be kept in their protective jacket and stored in the appropriate container according to the sensitivity of the data stored on them to prevent unauthorized access, damage, modification, or destruction.

4. If diskettes become defective and are to be destroyed, the media shoud also be reformatted, reinitialized, or deguassed before being shredded or placed in a container for destruction.

5. Diskettes containing sensitive information must be reformatted, reinitialized, or deguassed prior to reuse. Deleting or killing a file does not remove it from the diskette.

6. Backup copies of sensitive data should always be maintained and stored away from work areas. Backup copies of sensitive data must be protected in the same manner as the original data.

7. Diskettes will not be removed from the organization without the written approval of the ADPSSO.

8. On multiuser systems, each user should maintain his/her own diskettes. Data files maintained on a hard disk should be write protected or have password protection to avoid damage or destruction by other users.

9. As an item of US Government property, diskettes are subject to inspection/examination for the presence of unauthorized data or software.

APPENDIX J

SECURITY PROCEDURES
COPYRIGHTED SOFTWARE DISKETTES

1. The individual who is responsible (by hand-receipt) for the microcomputer will also be responsible for its associated software.

2. Unauthorized reproduction of copyrighted software violates Federal law and policy established by AR 27-60 (Patents, Inventories, and Copyrights) and AR 310-1 (Publications, Blank Forms, and Printing Management). As such, appropriate disciplinary action will be taken against any person found in violation of these policies.

3. Commercial software may only be copied under the following conditions and only when expressly permitted by vendor license agreements.

a. When preparation of a backup copy is permitted to protect the original from loss or damage. The backup copy should be tested to ensure a true duplicate of the original was made. The backup copy should then become the working copy. The original copy should be kept in a separate, secure location (except for those duplicate copies maintained at the alternate COOP sites).

b. When quicker access is achieved when software is accessed directly from RAM (random access memory) or hard disk. The original will not be loaded onto other computers unless authorized in vendor agreements.

c. When several computers operate as terminals on a network sharing a hard disk for software, data storage and data sharing, and rapid retrieval. There must be an additional copy of the software (personal computer software packages, not the operating system) located at the terminal site for each simultaneous user, unless otherwise specified in vendor license agreements.

d. Software in the public domain is excluded from the conditions of the above.

4. No commercial software will be removed from the organization without written approval from the ADPSSO.

5. Commercial software will not be used for private purposes.

6. Privately owned software will not be used on Government-owned equipment.

7. All commercial software (master and backup copies) will have a label affixed indicating the specific microcomputers authorized its use. Software will not migrate amoung computers unless appropriately authorized.

8. Licensed software will be properly registered with the supplier. For network operations, a single point of contact will be established to distribute software updates to all users.

9. Software will not be borrowed; however, software may be tested by others to determine future use, possible purchase, etc., only if expressly permitted in vendor license agreements.

1Ø. All copyrighted software should be hand-receipted for by the same person signed for the computer. A central point of contact should be established to reduce duplication.

11. Unless vendor license agreements specify dispoal procedures for obsolete software, the obsolete diskettes will either be shredded or burned and destruction recorded on DA Form 3964, or the most recent version of the obsolete software will be stored in a secure place.

12. The installation ADP system security manager will ensure these procedures are implemented and may supplement them as necessary.

APPENDIX K

SAMPLE PASSWORD RECEIPT

I hereby acknowledge personal receipt for the PASSWORD associated with my user account and USERID as listed below for the computer system. I understand that I am responsible for the protection of the password, will comply with instructions provided me, and will not divulge it to any unauthorized person. I further understand that I should report to an appropriate security officer (ADPSSO or TASO) any problem I may encounter in the use of the password or any misuse of passwords by other persons which may occur in my presence.

USERID: ______________

PASSWORD: ______________

Signature: ____________________

Date: ____________________

APPENDIX L

TELEPHONE BOMB THREAT REPORT FORM

INSTRUCTIONS: Be calm. Be courteous. Listen, do not interrupt the caller. Notify supervisor/security officer by prepared signal while caller is on line.

DATE

TIME

EXACT WORDS SPOKEN:

QUESTIONS TO ASK
1. When is the bomb going to explode?
2. Where is the bomb right now?
3. What kind of a bomb is it?
4. What does it look like?
5. Why did you place the bomb?

INFORMATION OBTAINED:

DETERMINE THE FOLLOWING
(Mark in the Appropriate Blocks):

IDENTITY:	Male		Female		Adult		Juvenile	Age
VOICE:	Loud	Soft	Deep	High	Raspy	Pleasant	Intoxicated	Other
ACCENT:	Local		Not Local		Foreign		Region	
SPEECH:	Fast	Slow	Distinct	Distorted	Stutter	Nasal	Slurred	Lisp
LANGUAGE:	Excellent		Good	Fair	Poor	Foul	Other	
MANNER:	Calm	Angry	Rational	Irrational	Coherent	Incoherent	Deliberate	Other
	Laughing		Emotional		Righteous		Intoxicated/Druged	
BACKGROUND:	Office Machines		Factory Machines		Bedlam	Trains	Animals	
	Music	Quiet	Airplanes	Voices	Mixed	Party	Street Traffic	

IMMEDIATELY AFTER THE CALL: Notify your supervisor/security officer as instructed. Talk to no one other than instructed by your supervisor/security officer. The MILITARY POLICE DESK is to be notified by the supervisor or commander of the involved activity (684-2111/3456).

RECEIVING TELEPHONE NUMBER

PERSON RECEIVING CALL

CAC&FL Form 719
1 Aug 84

Edition of 1 Aug 77 is obsolete.

DISTRIBUTION LIST

	No. Copies
Defense Technical Information Center ATTN: DTIC-TCA Cameron Station Alexandria, VA 22314	2
Commander US Army TRADOC Analysis Command Fort Leavenworth, KS 66027-5200 ATTN: ATRC ATTN: ATRC-ZD ATTN: ATRC-TD ATTN: ATRC-RM ATTN: ATRC-FA	5
Director US Army TRADOC Analysis Command Fort Leavenworth, KS 66027-5200 ATTN: ATRC-F ATTN: ATRC-FO ATTN: ATRC-FM ATTN: ATRC-FT ATTN: ATRC-FS ATTN: ATRC-FD ATTN: ATRC-FF	7
US Army TRADOC Analysis Command ATTN: ATRC-FO (Technical Info Center) Fort Leavenworth, KS 66027-5200	1